WHAT IS CLAIMED IS:

1. A method comprising:

a first peer sending a message to a second peer on a peer-to-peer network, wherein the message indicates that the first peer is requesting a session with the second peer;

the first peer sending a first public key to the second peer;

the second peer receiving the first message;

the second peer receiving the first public key;

the second peer determining if a session with the first peer is to be established in response to the message indicating the first peer is requesting a session with the second peer;

if it is determined that a session with the first peer is to be established:

the second peer generating a first session key from the first public key;

the second peer sending a message including the first session key to the first peer indicating that the second peer accepts the request for the session; and

the first peer receiving the message including the first session key; and

the first peer and the second peer using the first session key to encrypt and decrypt data exchanged between the first peer and the second peer

to provide secure exchange of said data between the first peer and the second peer on the peer-to-peer network.

2. The method as recited in claim 1, wherein the data comprises one or more chat messages.

3. The method as recited in claim 1, wherein the data comprises one or more files.

4. The method as recited in claim 1, further comprising, if it is determined that a session with the first peer is not to be established, the second peer sending a message to the first peer indicating that the second peer rejects the request for the session.

5. The method as recited in claim 1, further comprising:

if it is determined that a session with the first peer is to be established:

encrypting the message including the first session key on the second peer using the first public key prior to said sending the message including the first session key; and

decrypting the message including the first session key on the first peer using a private key corresponding to the first public key after said receiving the message including the first session key.

6. The method as recited in claim 1, further comprising:

ending the session between the first peer and the second peer;

establishing a new session between the first peer and the second peer subsequent to said ending the session; and

generating a second session key for the new session, wherein the second session key is different than the first session key; and

the first peer and the second peer using the second session key to encrypt and decrypt data exchanged between the first peer and the second peer in the new session to provide secure exchange of said data between the first peer and the second peer on the peer-to-peer network.

7. The method as recited in claim 6,

wherein said generating a second session key for the new session comprises:

the first peer generating a second public key;

the first peer sending the second public key to the second peer on the peer-to-peer network;

the second peer receiving the second public key; and

the second peer generating the second session key from the second public key.

8. The method as recited in claim 7, further comprising:

the second peer sending the second session key to the first peer; and

the first peer receiving the second session key.

9. The method as recited in claim 1, wherein the session is a chat session.

10. The method as recited in claim 1, further comprising:

a third peer sending a third public key to the first peer,; and

the first peer generating a third session key from the third public key, wherein only the first peer and the third peer possess the third session key.

11. The method as recited in claim 10, further comprising:

the third peer sending a fourth public key to the second peer; and

the second peer generating a fourth session key from the fourth public key, wherein only the second peer and the third peer possess the fourth session key.

12. The method as recited in claim 1, further comprising:

a third peer on the peer-to-peer network joining the session; and

providing the first session key to the third peer;

wherein the third peer is configured to encrypt messages to be sent to the first peer and to the second peer using the first session key, and wherein the third peer is further configured to decrypt encrypted messages received from the first peer and from the second peer using the first session key.

13. The method as recited in claim 1, wherein the first public key and an associated private key are generated using the RSA (Rivest-Shamir-Adleman) algorithm.

14. The method as recited in claim 1, wherein the first peer and the second peer are configured to operate in accordance with a peer-to-peer platform in the peer-to-peer network, wherein the peer-to-peer platform includes one or more protocols configured for use in communications among peers participating in the peer-to-peer network, and wherein the peer-to-peer platform further includes one or more policies that define rules and conventions for the peers participating in the peer-to-peer network, wherein the one or more protocols include a peer group discovery protocol configured for use by a peer in identifying a particular network region the peer is attached to and for discovering other peers attached to the particular network region.

15. A method comprising:

a first peer sending a first public key to a second peer in a peer-to-peer network;

the second peer receiving the first public key;

the second peer generating a first session key from the first public key;

the second peer sending the first session key to the first peer;

the first peer receiving the first session key; and

the first peer and the second peer using the first session key to encrypt and decrypt data exchanged between the first peer and the second peer to provide secure exchange of said data between the first peer and the second peer on the peer-to-peer network.

16. The method as recited in claim 15, wherein the data comprises one or more chat messages.

17. The method as recited in claim 15, wherein the data comprises one or more files.

18. The method as recited in claim 15, further comprising:

encrypting the first session key on the second peer using the first public key prior to said sending the first session key; and

decrypting the first session key on the first peer using a private key corresponding to the first public key after said receiving the first session key.

19. The method as recited in claim 15, further comprising:

ending the session;

sending a second public key from the first peer to the second peer in the peer-to-peer network;

the second peer receiving the second public key;

the second peer generating a second session key from the second public key, wherein the second session key is different than the first session key;

the second peer sending the second session key to the first peer; and

the first peer receiving the second session key;

wherein only the first peer and the second peer possess the second session key.

20. The method as recited in claim 15, wherein the first peer and the second peer are participants in a chat session on the peer-to-peer network.

21. The method as recited in claim 15, further comprising:

the first peer generating a third session key from a third public key of a third peer on the peer-to-peer network, wherein only the first peer and the third peer possess the third session key; and

the second peer generating a fourth session key from a fourth public key of the third peer, wherein only the second peer and the third peer possess the fourth session key.

22. The method as recited in claim 15, further comprising providing the first session key to a third peer in the peer-to-peer network, wherein the third peer is configured to use the first session key in encrypting messages to be sent to the first peer and the second peer and for decrypting encrypted messages received from the first peer and the second peer.

23. The method as recited in claim 15, wherein the first public key and an associated private key are generated using the RSA (Rivest-Shamir-Adleman) algorithm.

24. The method as recited in claim 15, wherein the first peer and the second peer are configured to operate in accordance with a peer-to-peer platform in the peer-to-peer network, wherein the peer-to-peer platform includes one or more protocols configured for use in communications among peers participating in the peer-to-peer network, and wherein the peer-to-peer platform further includes one or more policies that define rules and conventions for the peers participating in the peer-to-peer network, wherein the one or more protocols include a peer group discovery protocol configured for use by a peer in identifying a particular network region the peer is attached to and for discovering other peers attached to the particular network region.

25. A method comprising:

a plurality of peers in a peer-to-peer network joining in a session;

generating one or more session keys from one or more public keys of the plurality of peers, wherein the one or more session keys are configured for use by the plurality of peers to provide secure exchange of messages between peers in the session;

wherein there are one or more unique pairs of the plurality of peers, wherein each unique pair of the plurality of peers shares a particular one of the one or more session keys, wherein the particular session key is generated from a public key of one of the particular pair of peers, and wherein only the particular pair of peers possesses the particular session key; and

each of the one or more pairs of peers using the particular session key shared by the pair to encrypt and decrypt data exchanged between the peers in the pair to provide secure exchange of said data between the peers in the pair on the peer-to-peer network.

26. The method as recited in claim 25, wherein the data comprises one or more chat messages.

27. The method as recited in claim 25, wherein the public keys and associated private keys are generated using the RSA (Rivest-Shamir-Adleman) algorithm.

28. The method as recited in claim 25, wherein plurality of peers are configured to operate in accordance with a peer-to-peer platform in the peer-to-peer network, wherein

the peer-to-peer platform includes one or more protocols configured for use in communications among peers participating in the peer-to-peer network, and wherein the peer-to-peer platform further includes one or more policies that define rules and conventions for the peers participating in the peer-to-peer network, wherein the one or more protocols include a peer group discovery protocol configured for use by a peer in identifying a particular network region the peer is attached to and for discovering other peers attached to the particular network region.

29. A method comprising:

a plurality of peers in a peer-to-peer network joining in a session;

generating a session key from a public key of a first of the plurality of peers;

providing the session key to each of the plurality of peers, wherein only the plurality of peers in the session possess the session key; and

each of the plurality of peers in the session using the particular session key shared by the pair to encrypt and decrypt data exchanged between the peers in the session to provide secure exchange of said data among the peers in the session on the peer-to-peer network.

30. The method as recited in claim 29, wherein the data comprises one or more chat messages.

31. The method as recited in claim 29, wherein said generating a session key comprises:

the first peer sending the public key to a second of the plurality of peers; and

the second peer generating the session key.

32. The method as recited in claim 29, wherein plurality of peers are configured to operate in accordance with a peer-to-peer platform in the peer-to-peer network, wherein the peer-to-peer platform includes one or more protocols configured for use in communications among peers participating in the peer-to-peer network, and wherein the peer-to-peer platform further includes one or more policies that define rules and conventions for the peers participating in the peer-to-peer network, wherein the one or more protocols include a peer group discovery protocol configured for use by a peer in identifying a particular network region the peer is attached to and for discovering other peers attached to the particular network region.

33. A peer-to-peer network comprising:

a plurality of network nodes coupled to the peer-to-peer network;

a first peer configured to execute on one of the network nodes coupled to the peer-to-peer network;

a second peer configured to execute on a different one of the network nodes coupled to the peer-to-peer network;

wherein the first peer is configured to:

send a message to the second peer requesting a session with the second peer; and

send a first public key to the second peer;

wherein the second peer is configured to:

receive the first message requesting a session;

receive the first public key;

determine if a session with the first peer is to be established in response to the message requesting a session;

if the second peer determines that a session with the first peer is to be established:

generate a first session key from the first public key;

send a second message to the first peer, wherein the second message indicates that the second peer accepts the request for the session; and

send the first session key to the first peer;

wherein the first peer is further configured to:

receive the second message;

receive the first session key; and

wherein the first peer and the second peer are further configured to use the first session key to encrypt and decrypt data exchanged between the first peer

and the second peer to provide secure exchange of said data between the first peer and the second peer on the peer-to-peer network.

34. The peer-to-peer network as recited in claim 33, wherein the data comprises one or more chat messages.

35. The peer-to-peer network as recited in claim 33, wherein the data comprises one or more files.

36. The peer-to-peer network as recited in claim 33, wherein, if the second peer determines that a session with the first peer is not to be established, the second peer is further configured to send a message to the first peer indicating that the second peer rejects the request for the session.

37. The peer-to-peer network as recited in claim 33,

wherein the second peer is further configured to encrypt the first session key using the first public key prior to said sending the first session key; and

wherein the first peer is further configured to decrypt the encrypted first session key using a public key associated with the first public key after said receiving the first session key.

38. The peer-to-peer network as recited in claim 33, wherein the first peer and the second peer are further configured to:

end the session;

establish a new session between the first peer and the second peer subsequent to said ending the session; and

generate a second session key for the new session, wherein the second session key is different than the first session key; and

use the second session key to encrypt and decrypt data exchanged between the first peer and the second peer in the new session to provide secure exchange of said data between the first peer and the second peer on the peer-to-peer network.

wherein, in said generating a second session key, the first peer is further configured to:

generate a second public key; and

send the second public key to the second peer on the peer-to-peer network;

wherein, in said generating a second session key, the second peer is further configured to:

receive the second public key; and

generate the second session key from the second public key.

39. The peer-to-peer network as recited in claim 33, wherein the session is a chat session.

40. The peer-to-peer network as recited in claim 33, further comprising:

a third peer configured to execute on one of the network nodes coupled to the peer-to-peer network, wherein the third peer is configured to send a third public key to the first peer; and

wherein the first peer is further configured to generate a third session key from the third public key, wherein only the first peer and the third peer possess the third session key.

41. The peer-to-peer network of claim 40,

wherein the third peer is further configured to send a fourth public key to the second peer;

wherein the second peer is further configured to generate a fourth session key from the fourth public key, wherein only the second peer and the third peer possess the fourth session key.

42. The peer-to-peer network as recited in claim 33, further comprising:

a third peer configured to execute on one of the network nodes coupled to the peer-to-peer network, wherein the third peer is configured to:

join the session;

receive the first session key; and

encrypt messages to be sent to the first peer or the second peer using the first session key; and

decrypt encrypted messages received from the first peer or the second peer using the first session key.

43. The peer-to-peer network as recited in claim 33, wherein the first public key and an associated private key are generated using the RSA (Rivest-Shamir-Adleman) algorithm.

44. The peer-to-peer network as recited in claim 33, wherein the first peer and the second peer are configured to operate in accordance with a peer-to-peer platform in the peer-to-peer network, wherein the peer-to-peer platform includes one or more protocols configured for use in communications among peers participating in the peer-to-peer network, and wherein the peer-to-peer platform further includes one or more policies that define rules and conventions for the peers participating in the peer-to-peer network, wherein the one or more protocols include a peer group discovery protocol configured for use by a peer in identifying a particular network region the peer is attached to and for discovering other peers attached to the particular network region.

45. A peer-to-peer network comprising:

a plurality of network nodes coupled to the peer-to-peer network;

a first peer configured to execute on one of the network nodes coupled to the peer-to-peer network;

a second peer configured to execute on one of the network nodes coupled to the peer-to-peer network;

wherein the first peer is configured to send a first public key to the second peer;

wherein the second peer is configured to:

receive the first message;

generate a first session key from the first public key; and

send the first session key to the first peer; and

wherein the first peer is further configured to receive the first session key;

wherein the first peer and the second peer are further configured to use the first session key to encrypt and decrypt data exchanged between the first peer and the second peer to provide secure exchange of said data between the first peer and the second peer on the peer-to-peer network.

46. The peer-to-peer network as recited in claim 45, wherein the data comprises one or more chat messages.

47. The peer-to-peer network as recited in claim 45, wherein the data comprises one or more files.

48. The peer-to-peer network as recited in claim 45, further comprising:

wherein the second peer is further configured to encrypt the first session key using the first public key prior to said sending the first session key; and

wherein the first peer is further configured to decrypt the encrypted first session key using a public key associated with the first public key after said receiving first session key.

49. The peer-to-peer network as recited in claim 45,

wherein the first peer and the second peer are further configured to end the session;

wherein the first peer is further configured to send a second public key to the second peer;

wherein the second peer is further configured to:

receive the second public key;

generate a second session key from the second public key, wherein the second session key is different than the first session key; and

send the second session key to the first peer;

wherein the first peer is further configured to receive the fifth message including the second session key;

wherein the first peer and the second peer are further configured to use the second session key to encrypt and decrypt data exchanged between the first peer and the second peer in the new session to provide secure exchange of said data between the first peer and the second peer on the peer-to-peer network.

50. The peer-to-peer network as recited in claim 45, wherein the first peer and the second peer are participants in a chat session on the peer-to-peer network.

51. The peer-to-peer network as recited in claim 45, further comprising:

a third peer configured to execute on one of the network nodes coupled to the peer-to-peer network wherein the third peer is configured to send a third public key to the first peer;

wherein first peer is further configured to:

receive the third public key from the third peer; and

generate a third session key from the third public key;

wherein only the first peer and the third peer possess the third session key.

52. The peer-to-peer network of claim 51,

wherein the third peer is further configured to send a fourth public key to the second peer;

wherein the second peer is further configured to:

receive the fourth public key from the third peer; and

generate a fourth session key from the fourth public key;

wherein only the second peer and the third peer possess the fourth session key.

53. The peer-to-peer network as recited in claim 45, further comprising:

a third peer configured to execute on one of the network nodes coupled to the peer-to-peer network wherein the third peer is configured to:

receive the first session key; and

use the first session key for encrypting data to be sent to the first peer or the second peer and for decrypting encrypted data received from the first peer or the second peer.

54. The peer-to-peer network as recited in claim 45, wherein the first public key and an associated private key are generated using the RSA (Rivest-Shamir-Adleman) algorithm.

55. The peer-to-peer network as recited in claim 45, wherein the first peer and the second peer are configured to operate in accordance with a peer-to-peer platform in the peer-to-peer network, wherein the peer-to-peer platform includes one or more protocols configured for use in communications among peers participating in the peer-to-peer network, and wherein the peer-to-peer platform further includes one or more policies that define rules and conventions for the peers participating in the peer-to-peer network, wherein the one or more protocols include a peer group discovery protocol configured for use by a peer in identifying a particular network region the peer is attached to and for discovering other peers attached to the particular network region.

56. A carrier medium comprising program instructions, wherein the program instructions are computer-executable to implement:

a first peer sending a first public key to a second peer in a peer-to-peer network;

the second peer receiving the first public key;

the second peer generating a first session key from the first public key;

the second peer sending the first session key to the first peer;

the first peer receiving the first session key; and

the first peer and the second peer using the first session key to encrypt and decrypt data exchanged between the first peer and the second peer to provide secure exchange of said data between the first peer and the second peer on the peer-to-peer network.

57. The carrier medium as recited in claim 56, wherein the data comprises one or more chat messages.

58. The carrier medium as recited in claim 56, wherein the data comprises one or more files.

59. The carrier medium as recited in claim 56, wherein the program instructions are further computer-executable to implement:

encrypting the first session key on the second peer using the first public key prior to said sending the first session key; and

decrypting the first session key on the first peer using a private key corresponding to the first public key after said receiving the first session key.

60. The carrier medium as recited in claim 56, wherein the program instructions are further computer-executable to implement:

ending the session;

sending a second public key from the first peer to the second peer in the peer-to-peer network;

the second peer receiving the second public key;

the second peer generating a second session key from the second public key, wherein the second session key is different than the first session key;

the second peer sending the second session key to the first peer; and

the first peer receiving the second session key;

wherein only the first peer and the second peer possess the second session key.

61. The carrier medium as recited in claim 56, wherein the first peer and the second peer are participants in a chat session on the peer-to-peer network.

62. The method as recited in claim 56, wherein the program instructions are further computer-executable to implement:

the first peer generating a third session key from a third public key of a third peer on the peer-to-peer network, wherein only the first peer and the third peer possess the third session key; and

the second peer generating a fourth session key from a fourth public key of the third peer, wherein only the second peer and the third peer possess the fourth session key.

63. The carrier medium as recited in claim 56, further comprising providing the first session key to a third peer in the peer-to-peer network, wherein the third peer is

configured to use the first session key in encrypting messages to be sent to the first peer and the second peer and for decrypting encrypted messages received from the first peer and the second peer.

64. The peer-to-peer network as recited in claim 56, wherein the first public key and an associated private key are generated using the RSA (Rivest-Shamir-Adleman) algorithm.

65. The carrier medium as recited in claim 56, wherein the first peer and the second peer are configured to operate in accordance with a peer-to-peer platform in the peer-to-peer network, wherein the peer-to-peer platform includes one or more protocols configured for use in communications among peers participating in the peer-to-peer network, and wherein the peer-to-peer platform further includes one or more policies that define rules and conventions for the peers participating in the peer-to-peer network, wherein the one or more protocols include a peer group discovery protocol configured for use by a peer in identifying a particular network region the peer is attached to and for discovering other peers attached to the particular network region.